Exhibit 49

SW-SEC00000673

From: Brown, Timothy [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=A1BCD95116E84D6692DD89F9D55C5B7A-BROWN, TIMO]
Sent: 6/24/2020 4:11:57 PM
To: Johnson, Rani [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0ee57945f15e47b3abaa99a59170ad3f-Johnson, Ra]; Quitugua, Eric [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=227693e84bc0400b84364660f692bc85-Quitugua, E]; Flores, Mitchelle [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=699e88f33a114aa39d5c5a20dbae3ecd-Flores, Mit]; Holmberg, Rick [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a3c5e69002674a9e93947be117d2ea15-Holmberg, R]; Kemmerer, Joel [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=7001182857294219b50223772a1dd507-Kemmerer, J]
CC: Griffiths, Harry [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=ce100b97ef72483184628264bdaf0ae5-Griffiths,]; Vanhoose, Josh [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=295432f076cd4513b9186342fa37ff6a-Vanhoose, J]
Subject: RE: SDL and Orion Improvement Program

We will start an external audit of the OIP layer. Harry has been working with the team on the DOJ issue where this came up as a possibility.

From: Johnson, Rani <rani.johnson@solarwinds.com>
Sent: Wednesday, June 24, 2020 10:00 AM
To: Brown, Timothy <timothy.brown@solarwinds.com>; Quitugua, Eric <eric.quitugua@solarwinds.com>; Flores, Mitchelle <mitchelle.flores@solarwinds.com>; Holmberg, Rick <rick.holmberg@solarwinds.com>; Kemmerer, Joel <joel.kemmerer@solarwinds.com>
Subject: FW: SDL and Orion Improvement Program
Importance: High

Please investigate and advise on next steps.

From: Hess, Steven <steven.hess@solarwinds.com>
Sent: Wednesday, June 24, 2020 9:55 AM
To: Erway, Chris <chris.erway@solarwinds.com>; Yerasi, Chandrasekhara <Chandrasekhara.Yerasi@solarwinds.com>; Johnson, Rani <rani.johnson@solarwinds.com>
Cc: Calvert, Brian <brian.calvert@solarwinds.com>; Stovenour, Rob <rob.stovenour@solarwinds.com>; Morrill, Jeremy <Jeremy.Morrill@solarwinds.com>; Vrabel, Tomas <Tomas.Vrabel@solarwinds.com>; Gray, Paul <paul.gray@solarwinds.com>; Griffiths, Harry <Harry.Griffiths@solarwinds.com>; Schneeweiss, Petr <Petr.Schneeweiss@solarwinds.com>; Danner, Tim <Tim.Danner@solarwinds.com>
Subject: Re: SDL and Orion Improvement Program

Adding Rani and gave her an overview. She can pull in the security and WebOps teams to get this tackled and potentially take things offline to keep us safe.

Thanks,

solarwinds

Steven Hess | Director, SRE | ITOM
Office: 512.498.6076

From: "Erway, Chris" <chris.erway@solarwinds.com>
Date: Wednesday, June 24, 2020 at 9:13 AM
To: "Yerasi, Chandrasekhara" <Chandrasekhara.Yerasi@solarwinds.com>, "Hess, Steven" <steven.hess@solarwinds.com>
Cc: "Calvert, Brian" <brian.calvert@solarwinds.com>, "Stovenour, Rob" <rob.stovenour@solarwinds.com>, "Morrill, Jeremy" <Jeremy.Morrill@solarwinds.com>, "Vrabel, Tomas" <Tomas.Vrabel@solarwinds.com>, "Gray, Paul" <paul.gray@solarwinds.com>, "Griffiths, Harry" <Harry.Griffiths@solarwinds.com>, "Schneeweiss, Petr" <Petr.Schneeweiss@solarwinds.com>, "Danner, Tim" <Tim.Danner@solarwinds.com>
Subject: RE: SDL and Orion Improvement Program

+CC Steve, Harry, Petr

Has anyone done a security audit of the OIP server / api.solarwinds.com infrastructure to try and find out if OIP was compromised, for example by serving alternate XML files to one or more Orion installations?

Given that OIP hasn't been ruled out yet — out of an abundance of caution I recommend we seriously consider taking the OIP endpoints offline until it is ruled out. That would give us time to conduct a review and lock it down. (For example by securing the XML files and serving them elsewhere.)

Jeremy would be able to talk about the impact on sales and PM for tracking trial behavior daily, usage by paid customers, etc. But we could consider keeping the POST events endpoint up, if the system is able to run without GETting the latest XML files.

I'm just hearing of this potential attack vector for the first time, and it sounds risky to me to not consider disabling it immediately until we know more.

On Wed, Jun 24, 2020 at 9:20 AM, Chandrasekhara Yerasi <Chandrasekhara.Yerasi@solarwinds.com> wrote:

> SqlCommand.ExecuteNonQuery() is used to run the TSQL defined in the XML; so there is no restriction on the SQL commands that can be run.
>
> https://bitbucket.solarwinds.com/projects/PLATFORM/repos/orionimprovementclient/browse/Src/SolarWinds.OrionImprovement.BusinessLayer/Tasks/DatabaseQueryTask.cs
>
> The possible tasks that can be defined in the XML, parsed and run are at
>
> https://bitbucket.solarwinds.com/projects/PLATFORM/repos/orionimprovementclient/browse/Src/SolarWinds.OrionImprovement.BusinessLayer/Tasks
>
> Also WebOps team maintains these servers.

From: Vrabel, Tomas
Sent: Wednesday, June 24, 2020 7:39 AM
To: Yerasi, Chandrasekhara <Chandrasekhara.Yerasi@solarwinds.com>; Erway, Chris <chris.erway@solarwinds.com>; Gray, Paul <paul.gray@solarwinds.com>
Cc: Calvert, Brian <brian.calvert@solarwinds.com>; Stovenour, Rob <rob.stovenour@solarwinds.com>
Subject: RE: SDL and Orion Improvement Program

Yeah, and even more dangerous attack vector:

OIP XMLs contain SQL queries but I'm not sure whether it can contain also INSERT/UPDATE commands. If not, are we sure there is no workaround?

In case attacker can run arbitrary command in customer installation, nothing is easier than configure alert that always triggers with actions that will create some malicious vbs file (like reverse shell) and immediately execute it in other alert action.

From: Yerasi, Chandrasekhara
Sent: Wednesday, June 24, 2020 2:33 PM
To: Erway, Chris <chris.erway@solarwinds.com>; Gray, Paul <paul.gray@solarwinds.com>
Cc: Calvert, Brian <brian.calvert@solarwinds.com>; Stovenour, Rob <rob.stovenour@solarwinds.com>; Vrabel, Tomas <Tomas.Vrabel@solarwinds.com>
Subject: RE: SDL and Orion Improvement Program

DevOps and DBA maintain the OIP application and DB servers. Deployment to the OIP server for quire some years is basically deploying XML files and running DB scripts on the DB by DBA to store the new reported data.

The one attack path that we need to analyze and harden for the customer installations if the OIP server is compromised is the following - OIP client on the customer orion install downnloads updated OIP XML query files for installed modules (with basically SWQL/SQL queries that can be executed on the local system). The format of the files downloaded is "Module-Name.xml". Through this attack, they can definitely collect the data from the orion system.

We need to debate if we want to completely close this path and package updated OIP XML files with OIP client with product releases.

From: Erway, Chris
Sent: Wednesday, June 24, 2020 7:07 AM
To: Gray, Paul <paul.gray@solarwinds.com>
Cc: Calvert, Brian <brian.calvert@solarwinds.com>; Stovenour, Rob <rob.stovenour@solarwinds.com>; Vrabel, Tomas <Tomas.Vrabel@solarwinds.com>; Yerasi, Chandrasekhara <Chandrasekhara.Yerasi@solarwinds.com>
Subject: RE: SDL and Orion Improvement Program

Oh, yikes, I often forget that on-prem Orion already has a SaaS endpoint open to the public Internet — OIP. Sounds pretty important, I didn't realize it's possible an attacker could use it to take over all customer installations.

Is anyone from DevOps or BizApps involved in maintaining the server it runs on? Or is it historically architecture's responsibility?

On Wed, Jun 24, 2020 at 5:01 AM, Paul Gray <paul.gray@solarwinds.com> wrote:

> Tomas,
>
> Thanks for your help on this.
>
> Regards,
>
> Paul
>
> ---
>
> **From:** Vrabel, Tomas <Tomas.Vrabel@solarwinds.com>
> **Sent:** Wednesday, June 24, 2020 3:56 AM
> **To:** Gray, Paul <paul.gray@solarwinds.com>; Yerasi, Chandrasekhara <Chandrasekhara.Yerasi@solarwinds.com>
> **Cc:** Calvert, Brian <brian.calvert@solarwinds.com>
> **Subject:** RE: SDL and Orion Improvement Program
>
> I created https://jira.solarwinds.com/browse/PA-5625 to track this.
>
> Next week I'm PTO but in July I would like to make this happen. I will discuss with Chandra how to set this up, my goal is to set up security backlog, checkmarx, whitesource and tracking of security bugs.
>
> I need to check whether there is eng. team for OIP, if not I'm not sure how will actually fix found bugs. I will discuss this with Brian and we can talk about it with Core eng. leadership and come back with results.

From: Gray, Paul
Sent: Tuesday, June 23, 2020 11:37 AM
To: Vrabel, Tomas <Tomas.Vrabel@solarwinds.com>; Yerasi, Chandrasekhara <Chandrasekhara.Yerasi@solarwinds.com>
Cc: Calvert, Brian <brian.calvert@solarwinds.com>
Subject: RE: SDL and Orion Improvement Program

I don't believe we cover OIP today with the SDL, but we should.

It probably should be someone in your/Brian's team. I assume we are carrying it forward with Slingshot. If so, we should carve out some people to work on fixing OIP security other features.

Steps log Jira tasks in our backlog

Get an FSR going

Get CheckMarx going

Get WhiteSoruce going

Conduct FSR with all of the rest of Core

Regards,

Paul

From: Vrabel, Tomas <Tomas.Vrabel@solarwinds.com>
Sent: Tuesday, June 23, 2020 2:13 AM
To: Gray, Paul <paul.gray@solarwinds.com>; Yerasi, Chandrasekhara <Chandrasekhara.Yerasi@solarwinds.com>
Subject: SDL and Orion Improvement Program

Hi Paul, Chandra,

Who is maintaining OIP server now when Chandra moved to MSP please?

Do we have SDL process enforced for Orion Improvement Program server?

If SDL is not enforced for OIP, we should do it ASAP and consider additional actions to make sure that OIP is very well protected.

OIP API is not authenticated so it can accept content for any user, API is exposed externally so everybody can access it. If the OIP server is compromised, consequences can be disastrous – ranging from simple XXE attacks or collection of customer credentials to attacks like taking over all customer installations.

Background:

We are now dealing with customer security incident and our initial analyses indicated relation with OIP. After some analyses the relation with OIP is ruled out *for now*.

However during our analyses I found out that OIP server is using vulnerable library ICSharpCode.SharpZipLib.dll in version 0.58.5.452, there is public CVE https://nvd.nist.gov/vuln/detail/CVE-2018-1002208.

This raise strong suspicious that OIP server is not under SDL.

Thank you

Tomas